

## CLAIMS

Therefore, having thus described the invention, at least the following is claimed:

1        1.        A system for providing network-based firewall policy configuration and  
2        facilitation, comprising:

3                a firewall facilitation coordinator configured to receive a request to add an  
4        application not currently supported by a user's firewall policy, and to generate a time  
5        window during which a user can run the application; and

6                a policy modification agent adapted to communicate with the firewall  
7        facilitation coordinator, the policy modification agent configured to receive a firewall  
8        modification request from the firewall facilitation coordinator, to be aware of  
9        communications or packets observed by the firewall during the time window, and to  
10       modify the user's firewall policy.

1        2.        The system of claim 1, further comprises a firewall process adapted to  
2        communicate with the policy modification agent, the firewall process includes the  
3        user's firewall policy, a firewall communications or packet inspector and a firewall  
4        filter.

1        3.        The system of claim 2, wherein the firewall facilitation coordinator is further  
2        configured to decode and decrypt the firewall modification request, and further  
3        configured to authenticate the user before taking action on the request.

1        4.        The system of claim 3, wherein the firewall facilitation coordinate further  
2        comprises at least one of a secure transceiver, a firewall facilitation coordinator  
3        controller, a user notification authenticator, a user database, or a firewall policy  
4        configuration/modification window generator.

1        5.        The system of claim 4, wherein the policy modification agent further  
2        comprises at least one of a secure transceiver, policy modification agent controller,  
3        policy modifier, blocking history checker or blocking database.

1        6.        The system of claim 5, wherein the user exercises the application during the  
2        time window with that application transmitting/receiving communications or packets  
3        through the network-based firewall with communications or packets associated with  
4        the application passing through the network-base firewall unblocked.

1        7.        The system of claim 5, wherein during the time window, the policy  
2        modification agent via the firewall process examines communications or packets  
3        associated with the application and modifies the user's firewall policy such that the  
4        communications or packets are allowed to pass through the firewall process  
5        unblocked.

1        8.        The system of claim 1, further comprises a blocking history checker for  
2        checking communications or packets observed during the time window to be  
3        associated with the application in order to identify questionable communications or  
4        packets which are defined as those communications/packets or  
5        communications/packet types that are already part of the user's firewall policy or  
6        communications or packets previously blocked at times other than during the time  
7        window but which are now observed during the time window.

1        9.        The system of claim 8, wherein the policy modification agent is configured to  
2        not modify the user's firewall policy to include the questionable communications or  
3        packets.

1        10.       The system of claim 9, wherein the policy modification agent is configured to  
2        record the questionable communications or packet types in a blocking history  
3        database.

1        11.       The system of claim 10, wherein the policy modification agent is configured to  
2        send an acknowledgement of questionable communications or packet types recorded  
3        in the blocking history database to the user via the firewall facilitation coordinator.

1        12.       The system of claim 10, wherein the policy modification agent is configured to  
2        attempt to modify the user's firewall policy a configurable number of times and if

3 unsuccessful, to notify the user/customer to seek assistance or to notify appropriate  
4 personnel for assistance.

1 13. The system of claim 8, wherein the policy modification agent is further  
2 configured to group the types of questionable packets singly and in combination of  
3 two or more.

1 14. The system of claim 13, wherein the policy modification agent is further  
2 configured to prioritize the groups based on a likelihood that the groups will be  
3 required to be added to the firewall policy in order to allow the new application to  
4 function properly, and to label the groups in order of priority.

1 15. The system of claim 13, wherein the policy modification agent is further  
2 configured to perform successive policy modification attempts to remove previously  
3 added questionable packet groups and to add the next highest priority group to the  
4 firewall policy.

1 16. A method for modifying a firewall policy of a network-based firewall,  
2 comprising:

3 notifying a coordinating entity of a request to modify the firewall policy to  
4 incorporate filtering rules to allow communications or packets from a new application  
5 to pass through the network-based firewall without being blocked;

6 notifying a policy modifier of the modification request;

7 sending a user an indication of a time period during which the user can  
8 exercise a new application; and

9 examining the communications or packets traversing to/from the network-  
10 based firewall from/to the user and modifying the user's firewall policy such that  
11 necessary communications or packets associated with the new application are allowed  
12 to pass through the network-based firewall.

1 17. The method of claim 16, further comprising acknowledging the modification  
2 request and sending an acknowledgement of the modification request to a user's  
3 processing device.

1 18. The method of claim 16, further comprising authenticating the user before  
2 acting on the modification request.

1 19. The method of claim 16, wherein notifying a coordinating entity and a policy  
2 modifier of a request to modify a firewall policy step further comprises providing a  
3 name of the new application and a time frame for implementation of configuration  
4 change.

1 20. The method of claim 16, further comprising sending an acknowledgement of  
2 completion of the modification to the user's processing device.

1 21. The method of claim 16, further comprising blocking communications or  
2 packets not associated with filtering rules associated with the new application.

1 22. The method of claim 16, further comprising inspecting received  
2 communications or packets and checking a blocking history to identify questionable  
3 communications or packet types which are defined as those communications/packet  
4 types observed during the time window to be associated with the application but  
5 which are already included in the firewall policy or communications/packet types  
6 which were previously blocked at times other than during the time window but which  
7 are now observed during the time window.

1 23. The method of claim 16, further comprising modifying the firewall policy  
2 rules formed for the new application to provide for blocking the questionable  
3 communications or packets.

1 24. The method of claim 16, further comprising recording the questionable  
2 communications or packet types in a blocking history database.

1 25. The method of claim 16, further comprising sending an acknowledgement to  
2 the user's processing device to repeat an attempt to modify firewall policy when the  
3 new application does not function properly through the network-based firewall.

1       26.    The method of claim 16, further comprising notifying the user's processing  
2       device after a configurable number of repeat attempts that fail to modify the firewall  
3       policy such the new application can function properly through the firewall.

1       27.    The method of claim 16, further comprising allowing communications or  
2       packets associated with the new application to pass through the network-based  
3       firewall.

1       28.    The method of claim 22, wherein the examining step further comprises  
2       grouping the types of questionable packets singly and in combination of two or more.

1       29.    The method of claim 28, wherein the examining step further comprises  
2       prioritizing the groups based on a likelihood that the groups will be required to be  
3       added to the firewall policy in order to allow the new application to function properly,  
4       and labeling the groups in order of priority.

1       30.    The method of claim 28, wherein examining step further comprising  
2       performing successive policy modification attempts to remove previously added  
3       questionable packet groups and adding the next highest priority group to the firewall  
4       policy.

1       31.    A computer-readable medium for providing network-based firewall policy  
2       configuration and facilitation, comprising:

3            logic configured to notify a coordinating entity of a request to modify a  
4       firewall policy to incorporate filtering rules to allow communications or packets from  
5       a new application to pass through the network-based firewall without being blocked;

6            logic configured to notify a policy modifier of the modification request;

7            logic configured to send a user an indication of a time period during which the  
8       user can exercise a new application; and

9            logic configured to examine the communications or packets traversing to/from  
10      the network-based firewall from/to the user and modifying the user's firewall policy

11 such that necessary communications or packets associated with the new application  
12 are allowed to pass through the network-based firewall.

1 32. The computer-readable medium of claim 31, further comprising logic  
2 configured to acknowledge the modification request and logic configured to send an  
3 acknowledgement of the modification request to a user's processing device.

1 33. The computer-readable medium of claim 31, further comprising logic  
2 configured to authenticate the user before acting on the modification request.

1 34. The computer-readable medium of claim 31, wherein the logic configured to  
2 notify a coordinating entity and a policy modifier of a request to modify a firewall  
3 policy is further includes logic configured to provide a name of the new application  
4 and a time frame for implementation of configuration change.

1 35. The computer-readable medium of claim 31, further comprising logic  
2 configured to send an acknowledgement of completion of the modification to firewall  
3 facilitation coordinator and to the user's processing device.

1 36. The computer-readable medium of claim 31, further comprising logic  
2 configured to block communications or packets not associated with filtering rules  
3 associated with the new application.

1 37. The computer-readable medium of claim 31, further comprising logic  
2 configured to inspect received packets and logic configured to check blocking history  
3 to identify questionable communications or packet types which are defined as those  
4 communications or packet types already included in the firewall policy or  
5 communications or packet types which were previously blocked at times other than  
6 during the time window but which are now observed during the time window .

1 38. The computer-readable medium of claim 31, further comprising logic  
2 configured to modify the firewall policy rules formed for the new application to  
3 provide for blocking previously blocked communications or packets.

1 39. The computer-readable medium of claim 31, further comprising logic  
2 configured to inspect received communications or packets and to check a blocking  
3 history to identify questionable communications or packet types which are defined as  
4 those communications/packet types observed during the time window to be associated  
5 with the application but which are already included in the firewall policy or  
6 communications/packet types which were previously blocked at times other than  
7 during the time window but which are now observed during the time window.

8  
1 40. The computer-readable medium of claim 31, further comprising logic  
2 configured to modify the firewall policy rules formed for the new application to  
3 provide for blocking the questionable communications or packets.

1 41. The computer-readable medium of claim 31, further comprising logic  
2 configured to record the questionable communications or packet types in a blocking  
3 history database .

1 42. The computer-readable medium of claim 31, further comprising logic  
2 configured to send an acknowledgement to the user's processing device to repeat an  
3 attempt to modify firewall policy when the new application does not function properly  
4 through the network-based firewall.

1 43. The computer-readable medium of claim 31, further comprising logic  
2 configured to notify the user's processing device after a configurable number of repeat  
3 attempts that fail to modify the firewall policy such that the new application functions  
4 properly through the network-based firewall.

1 44. The computer-readable medium of claim 31, further comprising logic  
2 configured to allow the communications or packets associated with the new  
3 application to pass through the network-based firewall.

1       45.    The computer-readable medium of claim 37, further comprising logic  
2       configured to group the types of questionable packets singly and in combination of  
3       two or more.

1       46.    The computer-readable medium of claim 45, further comprising logic  
2       configured to prioritize the groups based on a likelihood that the groups will be  
3       required to be added to the firewall policy in order to allow the new application to  
4       function properly, and to label the groups in order of priority.

1       47.    The computer-readable medium of claim 45, further comprising logic  
2       configured to perform successive policy modification attempts to remove previously  
3       added questionable packet groups and to add the next highest priority group to the  
4       firewall policy.